Oral Testimony
of

Steven Cooper, Chief Information Officer, Department of Commerce

Before the U.S. House of Representative
Committee on Oversight and Government Reform

Thursday, June 9, 2016

Chairman Chaffetz, Ranking Member Cummings and members of the Committee, thank you for the opportunity to testify this morning.

I am Steve Cooper, Chief Information Officer for the Department of Commerce. It is my pleasure to address the Committee and update you on our work for a successful 2020 Census.

As you know, the Census Bureau faces an increasing set of challenges, including declining survey participation rates; increasing survey costs per household; funding uncertainty; and evolving cybersecurity threats. The Census Bureau continues working to ensure the necessary information technology—or "IT"—is in place to support the 2020 Census.

In November, I testified before many of you and spoke about a major enterprise initiative providing support to the 2020 Census – the Census Enterprise Data Collection and Processing – known as "CEDCaP". CEDCaP is an integrated and standardized suite of systems that will provide shared data collection and processing solutions across all Census Bureau operations.

Just weeks ago, the Census Bureau announced a major decision on that path on whether to use commercial software products or develop our own systems to collect and process data in the 2020 Census. After a comprehensive evaluation and an extensive analysis, we have determined that a hybrid approach – combining a commercial off-the-shelf (COTS) system with specific solutions developed by Census experts – will best meet our needs. The full CEDCaP "COTS Capability Assessment and Analysis Report" is available as well as the related 2020 Decision Memo.

During this same period, our in-house innovation and development teams have been hard at work developing test prototypes for the 2020 Census field tests. These

prototypes delivered key digital data collection system capabilities for data collection. This testing has been a critical part of the development process, allowing us to better understand how to re-engineer our business processes to save money during the 2020 Census. The work of the teams helped us develop and refine our requirements, and to make a well-informed evaluation of the COTS products.

Based on our final requirements, an analysis of the development and testing results and with input from experts at Carnegie Mellon University and the National Academy of Sciences, we decided on an integrated COTS platform that can supply functional solutions that incorporate innovations that we have developed in-house. This approach meets our data collection and processing goals for the 2020 Census and builds the infrastructure to support our censuses and surveys in the future.

Refining the systems we use for data collection and processing is a critical component of our proposal to save $5.2 billion in the 2020 Census when compared to the 2010 Census design. Meeting the schedules and timelines is key to preparing for the 2018 End-to-End Test, which will test the integration of all major operations and systems.

The Census Bureau continues to explore how best to employ cloud computing services to support the performance and scaling needs of 2020 Census systems, particularly for the internet self-response option that must support millions of users. We have acquired new talent and are currently working to enhance and increase our staff knowledge of cloud initiatives. We are in the process of building and establishing the governance and relevant processes, and currently establishing the appropriate contracting vehicles for Census Bureau needs. As part of this effort, we have drafted documents to include a Cloud Strategy, a Cloud Maturity Model, Cloud CONOPS, Consolidated Project Dashboard, and Cloud Readiness Checklist among others. We are poised to evaluate cloud candidates' compatibility with Census systems and applications before beginning migration or transition activities.

The Census Bureau is currently engaging in robust technical activities to innovate and fully transition to the Cloud. Proof-of-concept activities include performing integration, load, and penetration testing to validate results. We have collected lessons learned to incorporate high availability and redundancy in the cloud. We have sufficiently gained essential knowledge of Cloud Service Providers (CSPs) technology and are prepared for the migration and integration of additional capabilities. We intend to engage and acquire private sector expertise to partner

with Census to obtain cloud services and ensure overall system readiness for the decennial census.

Obviously, securing confidential data is a major concern for the Census Bureau. The Census Bureau uses an enterprise layered defense approach to protect its data and systems, utilizing:

- Department of Homeland Security-managed Einstein program to protect Internet traffic;
- Cloud service provider to protect against Distributed Denial of Service (DDoS) attacks;
- Intrusion detection systems and intrusion prevention systems;
- Segmented Census Bureau's network to isolate the internal network from systems that are Internet accessible.
- Risk management framework guidelines from the National Institute of Standards and Technology (NIST).

Census works very closely with their colleagues in the Department of Commerce (DOC) in addressing the various cybersecurity goals issued by DOC, the Office of Management and Budget (OMB), and the Department of Homeland Security (DHS). We participate in the DHS EINSTEIN program that detects and blocks threats at the federal network perimeter, and are working with DOC to onboard into the DHS Continuous Diagnostic and Mitigation (CDM) program that helps agencies identify vulnerabilities and other risk factors inside their networks. Census also has a rigorous program for the development and formal approval of secure configuration baselines and conducts automated scanning to look for unapproved baseline changes and security vulnerabilities.

Moreover, Census also has an active Computer Incident Response Team (CIRT) to investigate incidents that may be cybersecurity related. The CIRT has trained forensic specialists on staff who are involved in incident investigation and response as needed. In addition to DHS Einstein, Census also employs a layered defense strategy with the implementation of Census Intrusion Detection Systems, firewalls and anti-virus scanning. Furthermore, it is working on a contract to provide "brand protection" to monitor the internet for sites that mimic the Census Bureau.

Consistent with my testimony in November and based on my ongoing observations, the Census Bureau and the 2020 Census Program are well positioned and poised to leverage enterprise initiatives to realize significant efficiencies. Innovations in cloud computing, and cybersecurity continue to show great promise.

But to adequately implement these strategies and meet the challenges will require the best efforts of the Census Bureau and continued Congressional support.

I am deeply grateful for this opportunity to testify before this committee and share these observations, and I am pleased to answer any questions you may have.